



Lock Controller
CL-05.2

OPERATION MANUAL

CE EAC



Lock Controller *CL-05.2*

Operation Manual

CONTENTS

1	APPLICATION.....	3
2	OPERATION CONDITIONS.....	3
3	TECHNICAL SPECIFICATIONS	4
4	DELIVERY SET.....	5
4.1	Standard delivery set.....	5
4.2	Additional equipment supplied upon request:.....	5
5	PRODUCT DESCRIPTION	6
5.1	Design and operation	6
5.2	Signal parameters of OD control output	6
5.3	Signal parameters of “Door” and “DU” inputs	7
5.4	Signal parameters of the additional output	8
5.4.1	“Fire Alarm input”	8
5.4.2	Output.....	8
5.4.3	Synchronization	8
5.5	Choosing IP-address setting method.....	9
6	MARKING AND PACKAGING.....	10
7	SAFETY REQUIREMENTS.....	10
7.1	Installation safety.....	10
7.2	Operation safety	10
8	INSTALLATION.....	11
8.1	General instructions.....	11
8.2	Cables	11
8.3	Installation order	11
8.4	Powering	16
8.5	Connection via Ethernet network.....	16
9	CONFIGURATION	16
10	FIRMWARE UPDATE	16
11	OPERATION	17
11.1	ACM when operating as a part of ACS	17
11.2	Indication	19
11.3	Troubleshooting	19
11.3.1	Controller is not working	19
11.3.2	Controller is not recognized by the PC	19
12	TRANSPORTATION AND STORAGE	20
13	MAINTENANCE	21
	APPENDIX 1. Controller connection through PoE-splitter.....	22
	APPENDIX 2. Controller Web-interface. User Manual	24

Dear customers!

Thank you for purchasing PERCo lock controller.

Please follow instructions given in this Manual carefully and this quality product will provide many years of trouble-free use.

The *Operation manual* (hereinafter – the Manual) contains information on technical characteristics, design and operation principle of **CL-05.2 lock controller** and is aimed at providing a more complete use of the lock controller. *The Manual also contains sections on transportation, storage and installation of the lock controller.* The Manual is to be used together with operation documentation on other devices connected.

Abbreviations agreed in the Manual:

RC – remote control;
 OD – operation device;
 SZ – secured zone;
 ACM – access control mode;
 ACS – access control system.

1 APPLICATION

CL-05.2 lock controller (hereinafter – *controller*) is designed for managing one-way or two-way (having two controllers of this model installed) entrance point. Controller features built-in *HID* and *EM-Marine* proximity card reader and is able to control one electromagnetic or electromechanical lock.



Note:

Having two **CL-05.2** lock controllers installed for managing one two-way entrance point, it is necessary to use normally-closed (opened when energized) electromechanical locks as operation unit. Electromagnetic or normally-open electromechanical locks in this configuration can be used only with additional interposing relay installed.

Controller can be used as a standalone unit or as a part of **PERCo-Web** access control system. Controller management and configuration can be performed through built-in web-interface or **PERCo-Web** network Software.

2 OPERATION CONDITIONS

With regards to resistance to environmental exposure lock controller conforms to category NF4 as per GOST 15150-69 (operation in premises with climate control).

Lock controller can be operated within the following conditions:

Ambient air temperature.....from +1°C to +40°C
 Relative air humidity at +25°C.....max 80%

3 TECHNICAL SPECIFICATIONS

Rated operating voltage.....	12±1.2VDC
Consumption current	max 0.15 A
Power consumption	max 2 W
Number of controlled entrance points	1
Number of RC inputs	1
Proximity card types	<i>HID, EM-Marine</i>
Card reading distance at the rated operating voltage for different card types:	
for HID cards	min 5 cm
for EM-Marine cards.....	min 8 cm
Card reading distance with lock controller installed on metal surface:	
for HID cards	min 4 cm
for EM-Marine cards.....	min 7 cm
Lock controller connection interface standard.....	<i>Ethernet (IEEE 802.3)</i>
Number of users (proximity cards).....	from 10,000 to 50,000 (see Note)
Number of log events ¹	from 230,000 to 870,000 (see Note)



Note:

Possible options for allocating memory (see Appendix 2, Clause 3.4):

- 50,000 cards and 230,000 events – set by default,
- 40,000 cards and 390,000 events,
- 30,000 cards and 550,000 events,
- 20,000 cards and 710,000 events,
- 10,000 cards and 870,000 events.

Number of additional outputs ²	1
Mean lifetime	8 years
Electric shock protection class.....	III under GOST R IEC 730-1-94
Housing protection class	IP54 under EN 60529
Lock controller dimensions (without cable).....	145×50×20 mm
Lock controller weight	max 0.3 kg



Note:

Initially lock controller features: IP-address and MAC-address, stated in the product certificate and at the inner side of the product housing; subnet mask: 255.0.0.0; gateway IP-address: 0.0.0.0.

¹ If log event is overloaded, new events start replacing the old ones (events are deleted in blocks of 256).

² Additional output configuration variants are described in Section 5.4.

4 DELIVERY SET

4.1 Standard delivery set

Controller	1
Metal base	1
Jumper	1
Suppressor (15-18V)	1
Mounting kit:	
plastic dowels	4
screws	4
Package	1
Certificate	1
Operation manual	1

4.2 Additional equipment supplied upon request:

Power supply unit	1
PoE-splitter ¹	1

¹ **PoE-splitter** allows controller powering via *Ethernet* network. Splitter can be used with network commutators, supporting power transmission technology through PoE twisted-pair cable and is compatible with *IEEE 802.3af* standard.

5 PRODUCT DESCRIPTION

5.1 Design and operation

Controller is designed as a block of electronics in a plastic housing with three LED indicators at the front panel. Protection of electronics from the negative impact of the environment is provided by potting. *Ethernet* network connection cable and the cable for other lock controller connections are located on the housing back side.

Controller features: non-volatile memory; non-volatile RTC-timer (real-time clock) and sound indicator (piezoceramic radiator).

Controller features a built-in proximity card reader and operates with proximity cards of max 64-bit code. Types of compatible cards: *HID* and *EM-Marine*.

Controller provides connection via *Ethernet (IEEE 802.3)* interface with *TCP/IP (ARP, IP, ICMP, TCP, UDP, DHCP)* protocol stack support and **PERCo-Web** system communication protocol application layer support.

Using electromechanical locks, opened when energized, it is possible to use two controllers for managing one two-way entrance point (supporting zone changing).

Using **LB-** or **LBP-**series (production *PERCo*) electromechanical locks with terminal block, controller traces lock circuit condition, which allows omitting door sensor (reed switch) use. Door sensor is replaced by the lock terminal block.

Controller allows lock operation with the following devices:

- RC-button ("*Exit*");
- proximity card, presented to the controller;
- computer (when connected via *Ethernet* network and at the Software installation);
- emergency unlocking device ("*Fire Alarm*").

Apart from this it is possible to connect the following supplementary equipment:

- door sensor (reed switch);
- external light and sound (Alarm) indicator.

Controller as a part of ACS provides:

- operation in ACM: "*Open*", "*Control*", "*Closed*", "*Arming*";
- saving the set ACM in non-volatile memory in order to prevent its change at power loss/recovery;
- global zoning control function support;
- commissioning function support;
- verification function support;
- possibility of operation unit arming and disarming;
- sending signals to the central surveillance panel.

5.2 Signal parameters of OD control output

Controller features one OD control output: *Lock* (orange wire). Output type – open collector. OD connection scheme is provided on Fig. 3.

Output is used for OD control and has the following parameters:

maximum voltage direct current	30V
maximum current	1A

Control output can support potential and pulse modes of lock operation. The mode is chosen with OD "**Control output operation mode**" parameter.

At **potential** OD operation mode:

- During a single passage, output gets activated for the period of time, defined in Software by “**Time of holding in unlocked state**” parameter or until the passage completion.
- Having OD set for “*Open*” in ACM, output gets activated until the mode is changed.

At **pulse** OD operation mode:

- During a single passage, output gets activated for the period of time, defined by “**OD control pulse duration**” parameter. OD gets unlocked until passage completion.
- Having OD set for ‘*Open*’ in ACM, output gets activated for the period of time, defined by “**OD control pulse duration**” parameter. Output will be activated each time for this period of time in one second after OD gets normalized.

Door input activation using door sensor (reed switch) indicates passage completion. Using **LB-** or **LBP-**series electromechanical locks with terminal block, circuit break through lock terminal block indicates passage completion.

5.3 Signal parameters of “Door” and “DU” inputs

Controller manages the states of two inputs: *Door* (white wire) and *DU* (green wire). Connection scheme is given on Fig. 3. Inputs can be used as follows:

- “*Door*” – for door sensor connection (reed switch);
- “*DU*” – for RC-button connection (“*Exit*”).

Normally-open relay contact or a scheme with open collector output can serve as a control element. Control element is to provide the following signal characteristics:

control element – relay contact:

minimal commutated current max 1 mA
 closed contact resistance
 (considering connection cable resistance) max 300 Ohm

control element – scheme with open collector output:

closed contact voltage
 (low level signal, on controller input) max 0.8 V.



Note:

All the unconnected inputs are pulled to the power supply. In order to create a high level signal, all the input contacts (“*Door*” and “*DU*”) feature resistors with 2 kOhm, connected to the power line +3,3 V.

Activation of “*Door*” signal depends on its initial state description in “**Contact normal state**” parameter in the Software:

- if input is stated as “**Open**”, its activation is made by sending on it a low level signal regarding *GND* contact. In this case normally open relay contact or open collector output scheme can serve as the control element.
- if input is stated as “**Closed**”, its activation is made by removing a low level signal regarding *GND* contact from it. In this case normally open relay contact or open collector output scheme can serve as the control element.

Having **LB-** or **LBP-**series electromechanical mortise locks with terminal block installed, reed switch installation and *Door* input connection are not required. In this case lock terminal block serves as the door sensor. Activation is made by circuit break through terminal block, thus in the Software it is required to have “**Closed**” value set for “**Normal contact state**” parameter.

“*DU*” input is “normally open” (its initial state is not described in the Software); thus its activation is made by sending on it low level signal regarding *GND* contact.

5.4 Signal parameters of the additional output

Controller has one additional output (brown cable), which, depending on configuration, can be used as a *Fire Alarm* input (Section 5.4.1), as additional output (Section 5.4.2) or as a synchronization channel at simultaneous operation of two controllers (Section 5.4.3).

This output is designed as a transistor n-p-n collector. In order to operate as an input, it is connected to the power line +3.3 V through resistor with 4.7 kOhm resistance.

Choose additional output use variant in **PERCo-Web** Network Software. In order to set the output operation mode, set the value according to Table 1 in “**Type**” parameter of the “**Additional output**” controller resource.

Table 1. Output configuration in network Software

“Type” parameter value of the “Additional output” controller resource	Output operation mode
“Fire Alarm”	“Fire Alarm” input for emergency unlocking device (Section 5.4.1)
“Standard”, “Alarm generator”, “Security and fire alarm”	Control output for additional equipment (Section 5.4.2)
“Synchronizing”	Clock bus of two controllers simultaneous operation (Section 5.4.3)

5.4.1 “Fire Alarm input”

In “*Fire Alarm input*” mode the additional output is used for connecting emergency unlocking device (“*Fire Alarm*”). Connection scheme is given on Fig. 3.

Normally open relay contact or a scheme with open collector output can serve as a control element. Input signal parameters are the same as stated for *Door* and *DU* inputs (Section 5.3).

Sending control signal from (“*Fire Alarm*”) emergency unlocking device, connected to the controller on the input, OD gets unlocked and stays in that condition until signal removing. Indication block green passage grant indicator is ON. All control commands are ignored.

5.4.2 Output

In “*Output*” mode the additional output can be used for:

- external light and sound (Alarm) indicator connection,
- signal transfer to the central observation board,
- other additional equipment connection.

Connection scheme is given on Fig. 3.

Output signal parameters:

maximum voltage DC max 12 V
 maximum current max 0.25 A

5.4.3 Synchronization

In “*Synchronization*” mode the output is used for synchronization of the simultaneous operation of two controllers when two-sided entrance point is to be arranged. In this mode controller outputs are connected between each other. This allows avoiding *OD Breaking* event registration when making the passage in direction, opposite to the one, in which the controller is installed. Connection scheme is given on Fig. 4. In this case other equipment connection to the additional outputs is not allowed.

5.5 Choosing IP-address setting method

Controller IP-address setting method is chosen by jumper installation and removal on **XP1** output on the controller back side. Output configuration is given on Fig. 1.



Attention!

Jumper installation and removal should be performed on de-energized equipment only.

There are the following IP-address setting methods:

1. User mode. Jumper removed.
 - If the IP-address (gateway, subnet mask) has not been changed by the user, the controller will operate with the initial settings: IP-address and MAC-address are stated in the controller certificate on the controller board; subnet mask 255.0.0.0; gateway IP-address 0.0.0.0.
 - If the IP-address (gateway, subnet mask) has been changed, the controller starts to operate with the new settings immediately.



Note:

Controller network settings change is possible only from the PC through the Web-interface or from the Software. At that the controller and the PC are to be in one subnet.

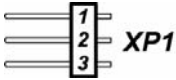
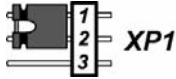
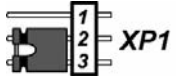
2. “*IP-MODE*”. 1–2 jumper position.
 - This mode is aimed at operation in networks with IP-address dynamic allocation. At that the controller gets the IP-address (gateway, subnet mask) from DHCP-network server/
3. “*IP-DEFAULT*”. 2–3 jumper position.
 - The controller operates with initial settings. IP-address and MAC-address are stated in the Controller certificate and on the controller board; subnet mask 255.0.0.0; gateway IP-address 0.0.0.0.
 - Controller access password is cleared.



Note:

User settings of the IP-address (gateway, subnet mask), in case they have been set, are saved when switching to “*IP DEFAULT*” mode. With next powering, if the jumper is removed, controller will start operating with these settings.

Table 2. Possible variants of jumper installation on XP1 output

No	Jumper position on XP1	Mode
1		User mode
2		“IP-MODE”
3		“IP-DEFAULT”

6 MARKING AND PACKAGING

Controller has a marking label located on the back side of the housing. The location of the label and other markers can be found on Fig. 1. The label features the following information about the controller:

- trademark and the manufacturer contact details;
- product name and model number;
- serial number;
- year and month of manufacture;
- power supply range;
- consumption current.

Apart from this, the back side of controller housing features labels with the initial:

- MAC – address;
- IP – address.

Controller is packed in a carton box keeping it safe from the damages during transportation and storage.

7 SAFETY REQUIREMENTS

7.1 Installation safety

Controller installation and maintenance should be carried out by qualified specialists who have studied this *Manual*.



Attention!

- Controller connection and jumper installation should be carried out with de-energized equipment and disconnected power supplies.
- Cabling should be executed with the general electrical and work safety rules observance.
- Controller installation should be carried out by fault-free instruments only.

Power supply installation safety requirements are provided in power supply operation Manual.

7.2 Operation safety

Controller operation should be carried out with the general electrical and work safety rules observance.



Do not use!

- Controller when power supply voltage does not comply with the technical characteristics described in Section 3 "*Technical specifications*".
- Controller in operation conditions that do not conform to those given in Section 2 "*Operation conditions*".

Power supply operation safety requirements are provided in power supply operation Manual.

8 INSTALLATION

Observe the instructions given in Section 7.1 during controller installation.

8.1 General instructions

It is recommended to install controller near OD. Controller should be installed at a place with easy access for proximity card presentation.

Controller should be installed at least 50 cm away from the readers and other controllers.

8.2 Cables

During controller installation, use cables given in Table 3.

Table 3. Cables used during controller installation

No	Connected equipment	Max. length, m	Type	Min. wire cross-section, mm ²	Example
1	Ethernet (IEEE 802.3)	100	Four twisted pair cables of no less than 5 th category	0.2	
2	Power supply	10	Twin cable	0.75	PVC isolation cord (2×0,75 two-colour)
3	OD – Lock	10			
4	RC-button	10	Twin cable	0.2	RAMCRO SS22AF-T (2×0,22) or CQR-2
5	Door sensor				
6	<i>Fire Alarm</i> device Additional equipment to the output				

The following requirements should be considered when laying all the signal cables (*Ethernet*, RC-button, door sensor and to the lock) and low-voltage power cables:

- it is recommended to install controller at least 1 meter apart from any other external readers and other EMI sources. EMI sources may reduce proximity card reading distance and be the cause of system operation malfunctions. The sources of electromagnetic interferences are: readers, AC lines, electric generators, electric motors, AC relays, thyristor light regulators, PC displays, computer and telephone signal communication lines;
- all signal cables, sensors, OD and low-voltage power cables should be laid at least 50 cm away from the alternating current cables, powerful motor control cables, pumps, drives, etc.;
- all signal cables can cross power cable only at a right angle;
- cable growth (except for *Ethernet* cable) is to be performed **with soldering only**.

8.3 Installation order

Follow the requirements given in Section 8.1. Controller connection should be carried out according to the scheme, given on Fig. 3, using the cables, given in Table 3. Follow this sequence during controller installation:

1. Unpack the box and check carefully controller delivery set according to Section 4. The equipment should be free of any mechanical damages.
2. Choose controller installation place. Follow the instructions given in Section 8.1 when choosing the installation place.

3. Mark and prepare holes on installation surface for the metal base mounting and for cabling as per scheme given on Fig. 2.
4. Loosen the screw located at the bottom side of controller housing and fixing it to the metal base. Remove the metal base.
5. Fix the metal base on the installation surface with four screws from the delivery set.
6. Choose controller IP-address setting method (Section 5.5) and install jumper on **XP1** output according to Table 2. if required. Jumper positioning is given on Fig. 1.
7. Pull controller cables through the cable hole on the installation surface. It is required to provide no less than 10 mm cable bend radius at the controller base during controller fixing. It is recommended to leave some spare cable length in order to retract controller from the wall and have access to the jumpers.
8. Install controller on the metal base and fix it with a screw in the bottom side of the housing.



Attention!

- If the connected *lock does not have the spark protection circuit*, it is required to use a spark protection diode (**VD1** on Fig. 3). For example, Schottky diode, used with operation current no less than 1A, of 1N5819 type.
- If the connected electromagnet *lock does not have demagnetizing circuit*, it is required to install the bidirectional suppressor from the delivery set. Suppressor is installed near the lock (**VD1** on Fig. 3).
- It is recommended to use only electromechanical locks during controller connection through PoE-splitter (instructions provided in Appendix), thus it is required to use the spark protection diode (**VD1** on Fig. 5) of 1N5819 type. It is **FORBIDDEN** to use suppressor in this case!

9. Prepare door for lock installation and install the lock in accordance with its operation documentation. Connect cable #3 (Fig. 3, Table 3) to the lock.
10. Ground lock housing or its locking plate in order to protect it from static electricity. If the lock is installed on the metal door, ground the door leaf. Grounding is to be performed with a wire of minimum 0.75 mm² cross-section.
11. Set the RC-button (“Exit”). RC-button installation place is to be chosen considering user access convenience (e.g. near the door). Connect cable #4 (Fig. 3, Table 3) to RC-button.
12. In case required, install magnet door sensor (reed switch). During installation, the magnet sensor should be fixed on the door frame and the magnet should be fixed on the door, providing stable sensor contact closing when the door is closed. Connection is made by cable #5 (Fig. 3, Table 3). Using **LB** or **LBP**-series electromechanical locks with terminal block, controller traces lock circuit condition, which allows omitting door sensor (reed switch) use. Door sensor is replaced by the lock terminal block. In this case controller *Door* input is to stay connected.
13. In case required, make the installation of the additional equipment (e.g. Alarm). Connect cable #6 (Fig. 3, Table 3) to the additional equipment.
14. Connect cables from the additional equipment to the standard controller cable according to scheme given on Fig. 3.
15. If simultaneous operation of two controllers for managing double-sided door is required, install and connect the second controller. Connection is made in parallel according to the cable colours (except for RC-button – usually it is not used and if needed, it can be connected separately to each of the controllers according to the scheme given on Fig. 3). Connection scheme is given on Fig. 4. Do not connect anything to the interconnected brown wires (SYNC).

**Note:**

Use normally closed electromechanical locks as an OD in this configuration. Electromagnet or normally open electromechanical locks can be used only having the interposing relay installed.

16. Connect Ethernet cable, coming from controller to the local network. Use RJ45 adapter from the delivery set and cable #1 in order to make an extension (Fig. 3, Table 3).

**Note:**

Controller power connection through PoE-splitter is given in Appendix 1.

17. Install power supply to its permanent operation position. Connect cable #2 (Fig. 3, Table 3) to the power supply and to the controller.
18. Lay and fix cables using plastic staples (e.g. SC4-6, SC5-7, SC7-10). During cable installation and cable laying it is necessary to consider the requirements given in Section 8.2.
19. Check lack of breaks and short circuits in all the lines.

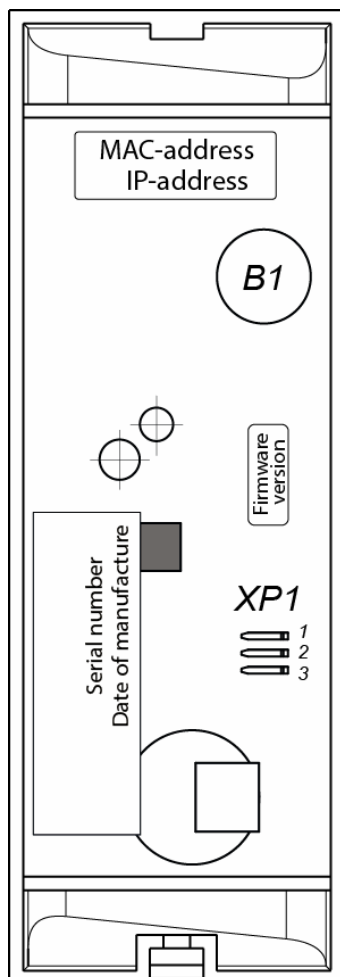


Figure 1. Controller back side outline

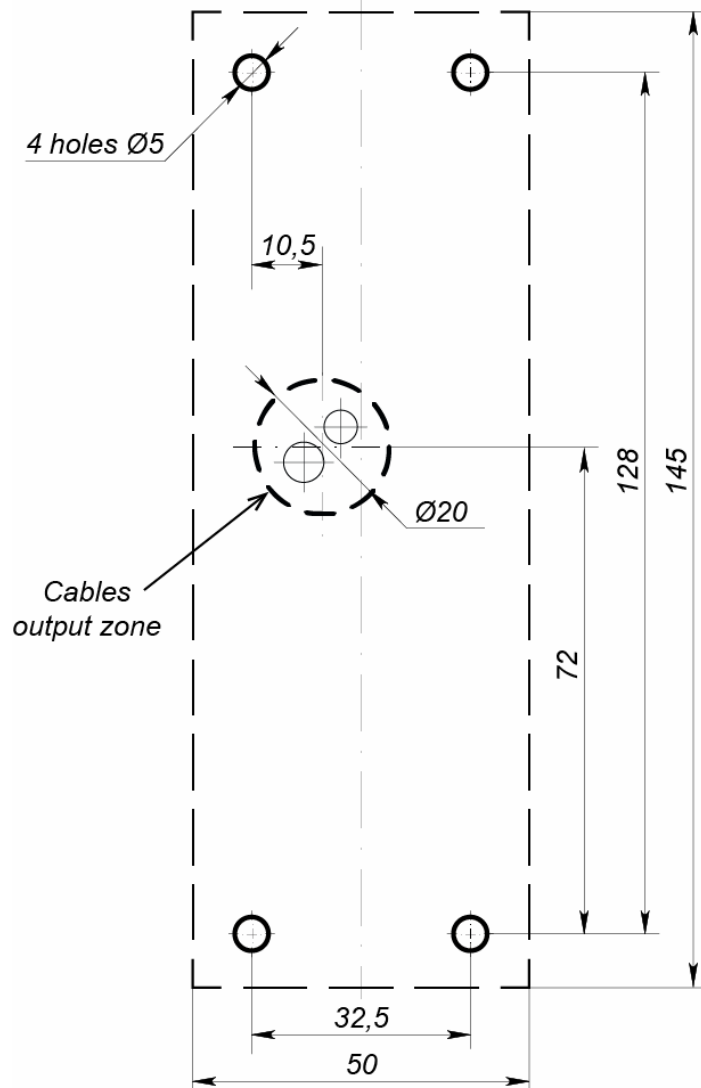
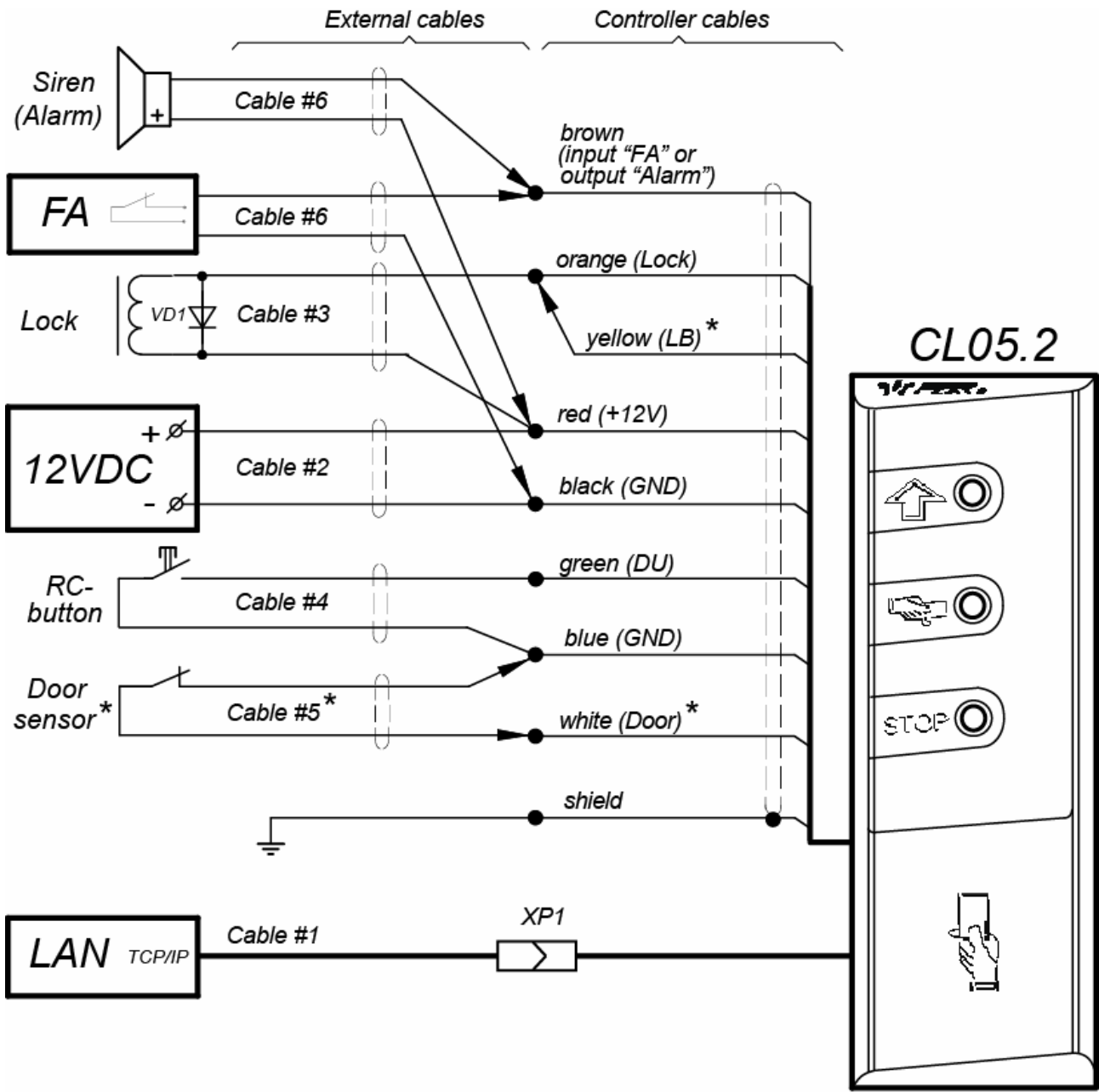


Figure 2. Hole spacing for controller installation (housing dimensions and a hole for cable laying are dotted)



Connector: XP1 - RJ45 (8P8C)

- * - when using locks with a contact group of the LB series:
 1) do not install the door sensor, do not connect the white wire,
 2) connect the yellow wire to the orange

Figure 3. Controller connection scheme

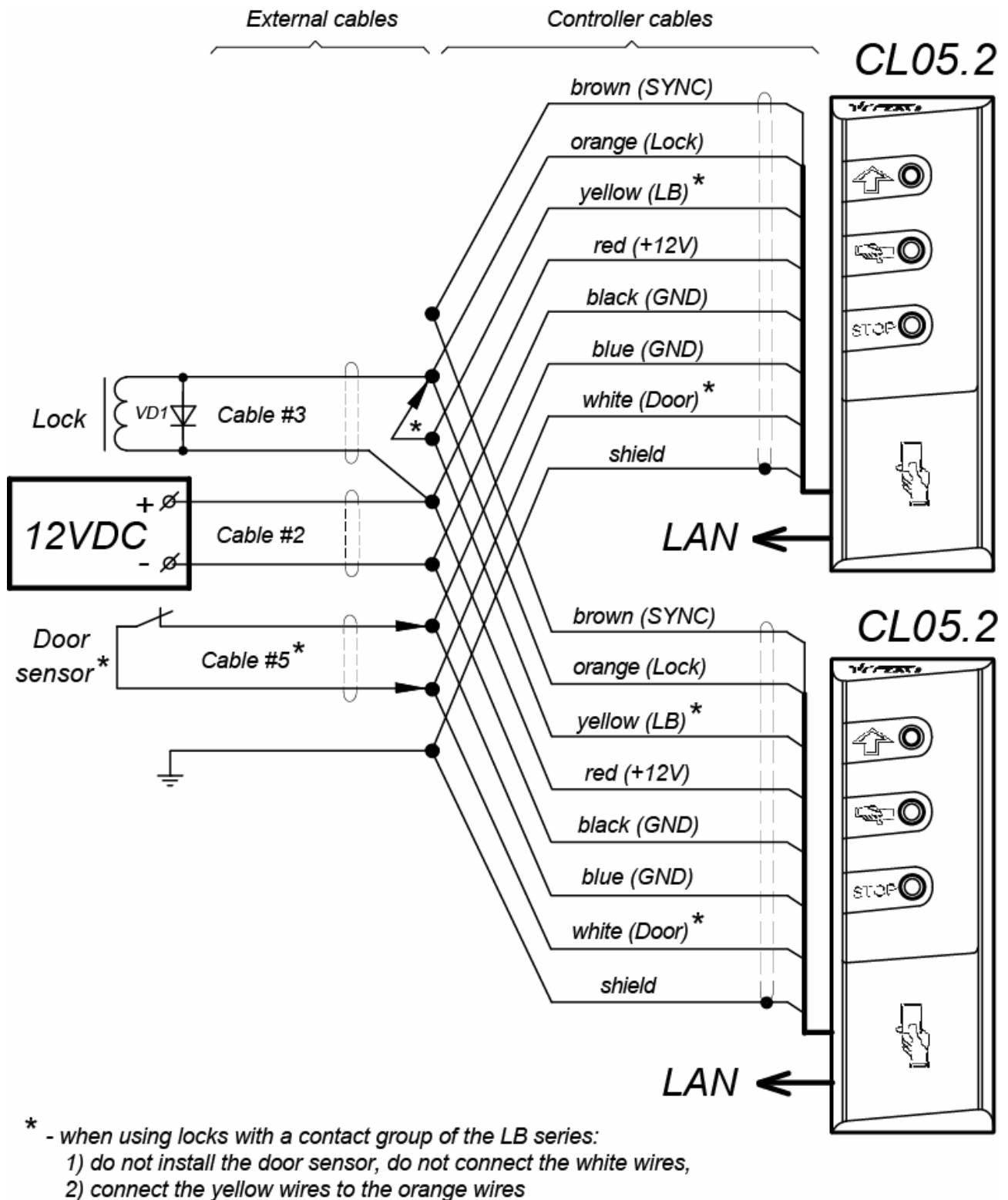


Figure 4. Scheme of the parallel connection of two controllers for managing double-sided door¹

¹ The given scheme features connection of locks, open when energized (normally closed electromechanical locks). In order to connect locks, open when de-energized (normally open electromechanical locks and electromagnet locks), install the supplementary relay with normally closed contacts connected to the lock power supply circuit.

8.4 Powering

When power supply is turned ON, all the light indicators on lock controller housing will start blinking for 3 seconds. After this period of time, controller indicators will show the latest ACM installed.

During controller first powering, after installation completion or after memory formatting, a simultaneous blinking of all the three indicators 2 times at a second will be initiated on the controller housing, indicating lack of controller settings. In this case configuration is to be transferred to the controller. This can be done through Web-interface or with the Software.

8.5 Connection via Ethernet network

On order to connect to the controller via *Ethernet* network, the computer is to be in one subnet with the controller. During the first connection computer network settings change may be required.

Initially all *PERCo* controllers feature IP-addresses from the 10th subnet, thus it is required to add IP-address to the additional parameters of computer TCP/IP: 10.x.x.x (x-random numbers) and subnet mask 255.0.0.0. Such servers and services as DNS and WINS are not required. Controller is to be connected to the same network segment or directly to the computer network card output.

When connection is made, all the network settings of the controller can be changed to the ones recommended by the system administrator from the Software or through Web-interface.

9 CONFIGURATION

Controller configuration, access cards transfer to the controller and a change of an ACM can be done:

1. through controller's Web-interface (see Appendix 2);
2. through Web-browser in *PERCo-Web* system;
3. by using the following local software, installed on the computer:
 - "Local software" **SL01** (license is not required);
 - "Local software with verification" **SL02**;



Note:

You can purchase additional software from authorized *PERCo* dealers. Also, the software, the licensing procedure and the electronic versions of the user's manuals on the software are available on the *PERCo* website at www.perco.com under "Support".

10 FIRMWARE UPDATE

Use "*Firming*" program to update the firmware and to format the *PERCo-Web* system controller memory. You can download the current version on our web-site www.perco.com.

You can also update the firmware and format the memory through the Web-interface of the controller in "**Diagnostics**" section (Appendix 3, Clause 9).

11 OPERATION

Observe safety instructions given in Section 7.2 during controller operation.



Do not!

- Use abrasive or chemically active materials for cleaning external surfaces of controller housing.
- Jerk and hit controller housing, lock, door sensor, RC-button and connecting cables in order to prevent their mechanical damage or deformation.

After configuration initiation controller can operate in the following modes:

Without connection to ACS (access control system) server

In case connection to *Ethernet* network and to the PC is unavailable, controller will start executing the following functions:

- Accepts presented cards identifiers from the built-in reader and, in accordance with their existence in the list, stored in controller memory, grants or bans the access.
- Controls the connected OD.
- Arms and disarms protective zones, controls OD in “*Arming*” ACM; activates additional output in “*Alarm*” mode.
- Fixes events in the controller memory event log.
- Supports passage time control and commissioning function.

Global zoning control function becomes available when controller is connected to the network and when connection with other system controllers is provided.

Connecting to the PC with “*Local Software*” installed:

- Events from log event are automatically relocated into programme database each time the programme is initiated. The data can be also relocated by clicking on the corresponding button in the programme.
- Data on identifier owner (full name) are stored in programme database.
- Verification is available in case “*Local Software with verification*” is installed.

Connected to ACS (access control system) server

Apart from the functions, supported during standalone operation, the following functions also become available:

- Data from the log event get automatically relocated into security system server database.
- Verification function is available depending on network Software modules installed.

11.1 ACM when operating as a part of ACS

ACM change is performed by the simultaneous order from the Software to both passage directions.

Controller as a part of ACS provides the following ACM through OD (ACM indication is given in Table 4):

“*Open*” ACM – free passage mode.

- OD gets unlocked until ACM change.
- RC-button (“*Exit*”) pressing is ignored.

“*Control*” ACM – main operation mode as an ACS element.

- OD is blocked.

- Presenting the access card, meeting all the passage grant criteria, to the reader. OD gets unlocked for **“Time of holding in unlocked state”**.

“Closed” ACM – passage ban mode.

- OD is blocked until ACM change.
- RC-button (“Exit”) pressing is ignored.
- Any access card presentation is registered as ACM violation.

“Arming” ACM

- OD is blocked until ACM change.
- RC-button (“Exit”) pressing is ignored.
- Protective zone arming, including OD.
- Arming / Disarming can be made by double presentation of the access card, having corresponding rights, to the reader.
- Passage through OD (OD breaking) switches protective zone, including OD, into “Alarm” mode.

Table 4. Controller indication

Card presentation		ACM	Indicators			
			Green	Yellow	Red	Sound, s
No configuration		No	5 Hz	5 Hz	5 Hz	Off
No		“Open”	On	Off	Off	Off
		“Control”	Off	On	Off	Off
		“Arming”	Off	1 Hz	1Hz	Off
		“Closed”	Off	Off	On	Off
Card has no access rights		“Open”	On	Off	Off	0.2
		“Control”	Off	Off	On	0.5
		“Arming”				
Any card		“Closed”				
Card has access right		“Open”	On	Off	Off	0.2
		“Control”				
		“Arming”	Off	Off	On	0.5
Card has access and arming/ disarming right		“Open”	On	Off	Off	0.2
		“Control”				
		“Arming” ¹				
Repeated presentation of the card with arming right	At taking (switch to “Arming” ACM)	“Arming”	Off	1 Hz	1Hz	0.2
	At non-taking ² (until return to the initial ACM)	“Open”	Off	Off	1sec	1
		“Control”				
Verification/ commissioning waiting time		Any	Off	2 Hz	Off	0.2

¹ Presentation of card having disarming rights in “Arming” ACM leads to: protective zone removal, including OU disarming and OU unlocking for **“Time of holding in unlocked state”**. After this period of time controller switches to ACM, set before protective zone arming (“Open” or “Control”; in case the previous ACM was “Closed”, then it switches to “Control” ACM).

² Sound and light indication is ON for 1 sec.

11.2 Indication

Possible variants of ACM indication, controller states and reactions to identifier presentation are given in Table 4. Indication is located on the indication module, featuring three light indicators on the controller housing front panel.



Note:

- During access card identifier reading in any ACM, sound signal 0.2 sec. long is sent, yellow light indicator changes its state for 0.2 sec. Other indicators state does not change.
- Having card access granted, light indication is on for “**Time of holding in unlocked state**” or until passage completion. If the passage is banned, indication will be ON for 2 sec.

11.3 Troubleshooting

Possible faults to be corrected by the customer themselves are given below. Contact the manufacturer if other fault or malfunction occurs.

11.3.1 Controller is not working

Possible causes of the controller malfunction are as follows:

1. **Power supply malfunction** – check the power supply.
2. **Malfunction of the equipment, connected to controller outputs** (lock, door sensor, RC-button) – make sure the connected devices are faultless.
3. **Faulty controller connection lines of other devices** – make sure the connection lines are operable.
4. **Faulty radio components on the controller board** – the controller needs repair at the manufacturer.

11.3.2 Controller is not recognized by the PC

Possible causes of the malfunction:

1. **No network settings in the computer** – set computer IP-address and subnet mask. Computer is to be connected either directly to the computer network card network connector or to the same Hub/Switch to which the computer is connected.
2. **Incorrect controller password has been used.** In the Software check correctness of the password used.
3. **Computer malfunctions** (with the Software, with databases, etc.).

Diagnostics of this malfunction is made by initiating the following command:

```
ping x.x.x.x
```

where x.x.x.x – IP-address of the controller.

If there is connection, you will see the following lines:

```
Answer from x.x.x.x: number of bytes=32 time<10mc TTL=128
```

If there is no connection (answer), check the correctness of routing sets in your network.

4. **Malfunctions of Ethernet network equipment**, HUB located between computer and controller, SWITCH and other network equipment including connection cables.

Diagnostics of this malfunction is made by initiating the following command:

```
ping x.x.x.x -l 576
```

where x.x.x.x – IP-address of the controller.

If there is connection and the standard minimal packet (576 bytes) is not fragmented, you will see the following lines:

```
Answer from x.x.x.x: number of bytes=576 time<10mc  
TTL=128
```

In this case it can be said that IP-packets are not fragmented to the size smaller than 576 bytes and the chosen connection should function correctly.

If it is impossible to get the positive answer, this means that on the IP-packet route there is a network commutating equipment, fragmenting IP-packets up to the size smaller than 576 bytes. Check the settings of this equipment and, if possible, increase *MTU* size. Usually this parameter is marked as *MaxMTU* or *IPMTU*.

5. **If several variants of commutation are possible**, use this command.

```
ping x.x.x.x -l 576 -t
```

Commutating in different ways, look at the response time, choosing the connection, giving the quickest response time.

6. **Controller malfunctions.** Faulty operation of the elements, providing connection via *Ethernet (IEEE 802.3)* interface.

If controller does not detect connection to *Ethernet*, connect it to the cable, from which another controller operates. If controller does not detect connection to *Ethernet* or connection with it cannot be restored, i.e. this controller is to be sent back to the manufacturer for diagnostics.

12 TRANSPORTATION AND STORAGE

Controller in the original package should be transported in closed freight containers or other closed type cargo transport units.

The storage of the controller is allowed indoors at ambient temperature from -20°C to +40°C and relative air humidity up to 98% at +25°C.

13 MAINTENANCE

Operation and technical staff, responsible for controller technical maintenance, is to know its design and operation rules.

Follow the rules given in Section 7 “*Safety requirements*” of this Manual when making any works on technical maintenance.



Attention!

- Disconnect controller from the power supply before making technical maintenance works.
- Test equipment is to be checked beforehand.

Once in three months maintenance operations made on scheduled basis according to program #1 are to be made. List of works is given in Table 5. Reports on technical maintenance works made on regularly scheduled basis are to be put in the scheduled works register book.

It is necessary to observe interval, technological order and methodic of scheduled works execution.

**Table 5. List of works to be made on regularly scheduled basis #1
(technological card #1)**

Type of works	Execution order	Equipment, instruments, materials	Norms and observed phenomena
1 Exterior check ; controller and power supply cleaning	1.1 Disconnect power supply from AC mains and remove dust, dirt and damp from all controller surfaces.	Cleaning waste, brush grainer.	No signs of dirt and damp.
	1.2 Remove covers from the power supply. If there is a reserve power supply (accumulator), remove any dust, dirt, damp and oxides from the terminals. Check the reserve power supply voltage. If needed, charge or change the battery.	Screwdriver, cleaning waste, brush grainer, C4352 indicator.	Voltage is to comply with data given in the battery certificate (min 12,6 V).
	1.3 Remove dust, dirt and corrosion from jumper contact surfaces and from the safety fuse.	Cleaning waste, brush grainer, benzine B-70.	No corrosion stains, no dirt.
	1.4 Check the rated value and OD safety fuse operability.		
	1.5 Check all the external circuit connections.		Connections are to comply with the scheme.
	1.6 Recover connection, in case the wire has been broken. Change the wire if isolation has been damaged.		No isolation damages and no wire breaks.
2 Normal operation check	2.1 Check controller operability as per Section 11.		Controller indication according to Section 11.2. Signal forming on the output according to its configuration.

Technical maintenance of other devices, connected to the controller, is given in operation documentation for these devices.

APPENDIX 1. Controller connection through PoE-splitter



Attention!

- Instruction provided refers to the splitters included in additional equipment delivery set.
- Total power consumption of the controller and of all the devices powered by it should not exceed 12 W. It is also recommended to leave min 10% reserve power.

Splitter description

PoE-splitter (hereinafter – *splitter*) is designed for energizing equipment, connected via *Ethernet* network. Splitter operates with any network commutators (hereinafter – *Switch*), supporting technology of electric power transmission via *PoE* twisted pair wire and compatible with *IEEE 802.3af* standard.

Splitter is designed as a block of electronics in a plastic housing featuring the following outputs:

Con 1 – output for *Ethernet* cable from *Switch* connection.

Con 2 – output for *Ethernet* controller cable connection;

Con 3 – power output for controller power cable connection.



Note:

For some models of splitters output voltage is chosen with the switcher. Operating with **PERCo** equipment it is necessary to turn the switcher into “12V” mode.

Connection sequence

Follow this sequence during controller connection through splitter:

1. Choose splitter installation place. Do not install splitter at more than 2 m distance from the controller.
2. Connect *Ethernet* cable from controller to **Con2** output of the splitter (Table 3).
3. Connect controller power-supply circuits to **Con3** output of the splitter. Connection scheme is given in Fig. 5 (other connections are to be made according to Fig. 3, Fig. 4, attachment plug for connection to the output is included into splitter delivery set).



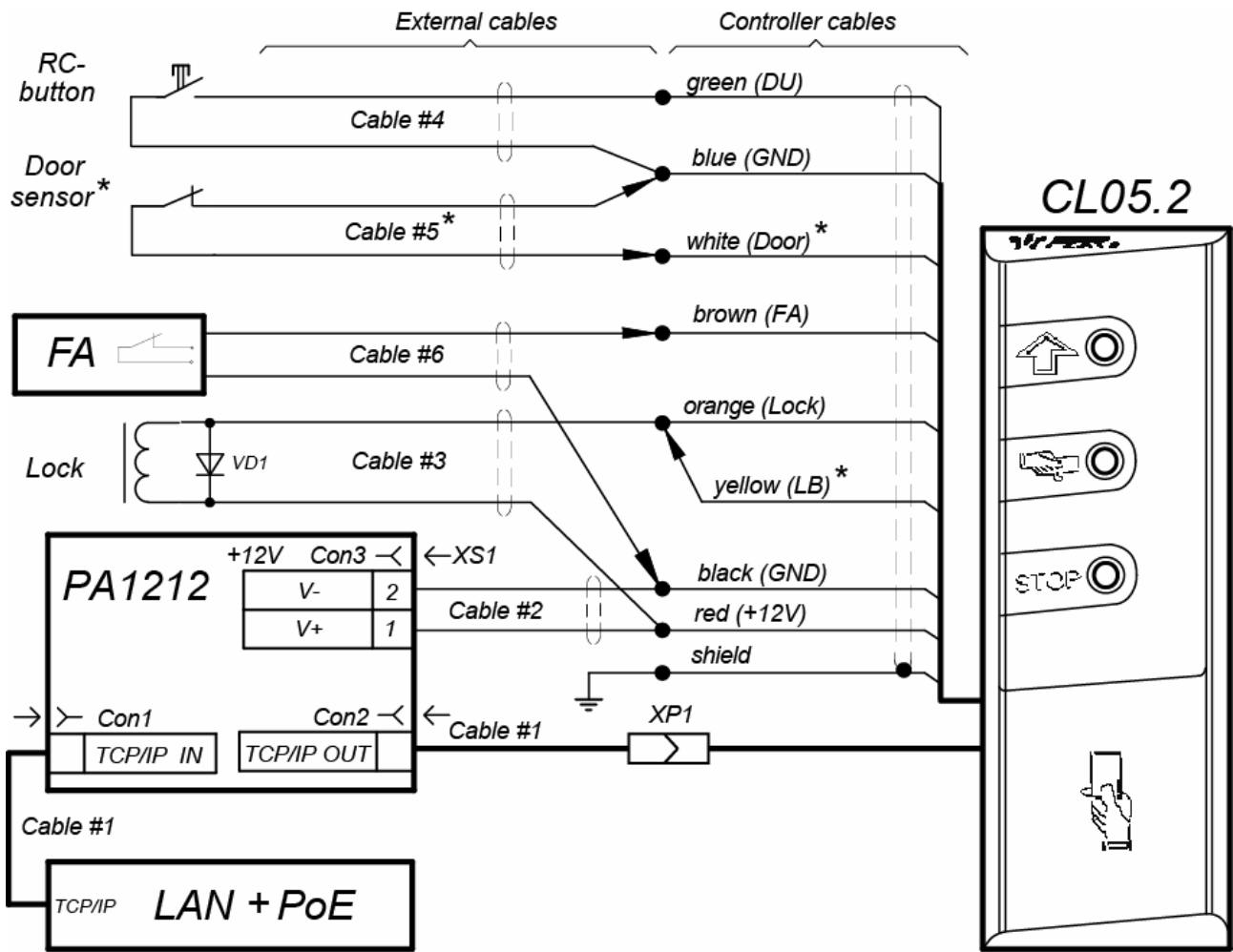
Attention!

It is **OBLIGATORY** to install a spark protection diode **VD1** (Fig. 3, Fig. 4) of 1N5819 type during lock connection. **DO NOT** use suppressors instead of spark protection diodes. It is recommended to use electromechanical locks only.

4. Connect *Ethernet* cable from *Switch* to **Con1** output of the splitter.

5. After verification between *Switch* and splitter, controller will be energized.

Disconnect *Ethernet* (coming from *Switch*) cable from **Con1** output of the splitter to de-energize controller.



Connectors: XP1 - RJ45 (8P8C),
XS1 - DC2.5/5.5

- * - when using locks with a contact group of the LB series:
 1) do not install the door sensor, do not connect the white wire,
 2) connect the yellow wire to the orange

Figure 5. Controller connection scheme through PoE-splitter

APPENDIX 2. Controller Web-interface. User Manual

CONTENTS

1.	WEB-INTERFACE OPPORTUNITIES	25
2.	CONNECTION TO WEB-INTERFACE OF THE CONTROLLER	25
3.	SETTING.....	27
3.1	Change of network setting of the controller	27
3.2	Setting of the access password of the controller	27
3.3	Change the system time of the controller	27
3.4	Choice of Settings of memory allocation	28
4.	CONFIGURATION	28
4.1	The choice of the controller configuration.....	28
4.2	Configuration of the Settings of the controller resources	29
4.2.1	Operating devices.....	29
4.2.2	Physical contacts (inputs and outputs)	30
4.2.3	Readers	31
4.2.4	The reading format of the card identifiers	31
4.2.5	Internal responses	31
5.	CONTROL OF OPERATING DEVICE	32
6.	ACCESS CARDS	33
6.1	Entering of the cards identifiers	33
6.2	The list of stored cards	34
6.3	Loading the identifiers from a file.....	36
7.	EVENTS	37
8.	STATUS	38
9.	DIAGNOSTICS.....	38

1. WEB-INTERFACE OPPORTUNITIES

Using Web-interface without installation of additional software allows performing following steps for the controller and connected devices:

- Change configurations, access password and time of built-in clocks of the controller.
- Configure Settings of operational device, readers and other equipment's of the controller.
- Set ACM for controller and operation devices.
- Record the access card numbers in the controller memory, assign them the rights for arming or disarming.
- Monitor event log of the controller and save them as a file.
- Control the status of the controller and connected devices, monitor the event log.
- Troubleshoot the controller, format the memory and update the embedded software.



Attention!

It is possible only with the Web-interface select controller configuration and Settings of built-in memory (access cards/events).



Note:

Change of configurations via Web-interface of the controller is not available if the controller is under control of network or local software of **PERCo** systems (you can only monitor the configuration; operations are forbidden). The access to Web-interface is allowed if the software is configured to “**Allow Web-interface**”. It is possible after stopping the operation of the software and stopping the server of **PERCo** system.

2. CONNECTION TO WEB-INTERFACE OF THE CONTROLLER

Connection between the controller and the computer is performed via *Ethernet* interface (IEEE 802.3). Make sure that the computer and the controller are on the same subnet *Ethernet*. It may become necessary to change network settings of the computer, browser settings and to check operation of the network. IP-address of the controller is specified in the certificate and the controller board.

To connect the controller to Web-interface:

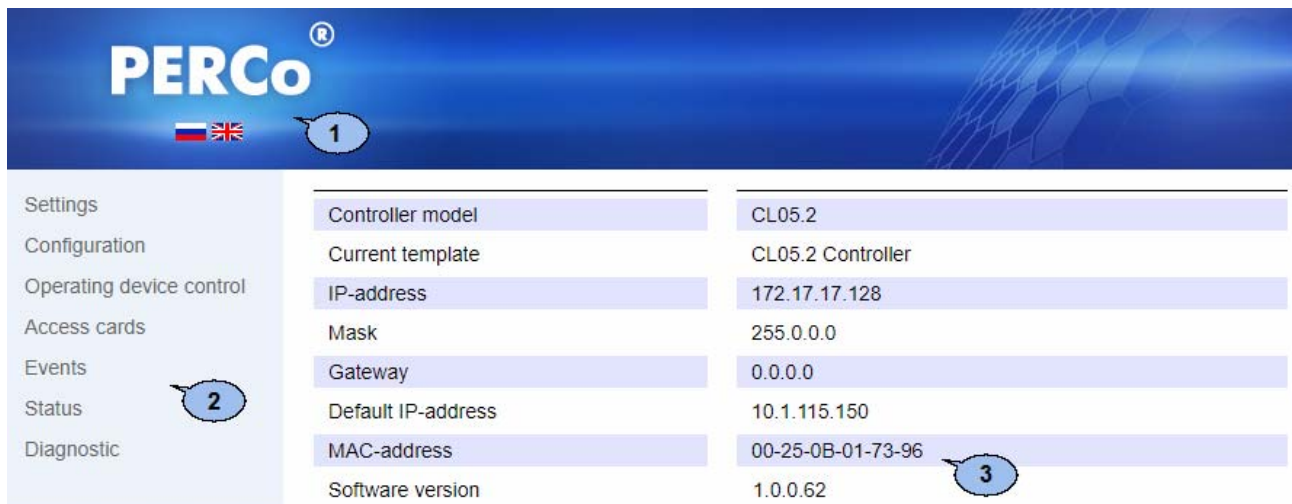
1. Open Web-browser (e.g. *Internet Explorer*).



Note:

Web-interface was tested with the Web-browsers: *Microsoft IE* version 10 or higher, *Google Chrome* version 32 or higher, *Mozilla Firefox* version 32 or higher, *Opera* version 30 or higher, *Microsoft Edge* and for *MacOS Apple Safari* 9 or higher. If you use other browsers and outdated versions, malfunctions of the Web-interface can appear.

2. Enter in the address bar IP-address of the controller and press the button “**Enter**” on the keyboard. If necessary, enter the access password to the controller. By default, there is no password. When entering the password, the content of the field “**User name**” doesn't matter.
3. After that the main Web-page of the controller interface is opened. At the home page are displayed the model, configuration, network settings of the controller and the version of embedded software. Every time when you open the main page, current data read from the controller are displayed there.



On the page, you can select following:

1. The title bar if he page contains **PERCo** trademark and buttons to select the language of Web-interface. By clicking on the **PERCo** company logo you navigate to the main page from other sections of Web-interface.
2. Sidebar of the Web-interface navigation. The panel has the following structure

<i>“Settings”</i>	<i>“Network”</i>	
	<i>“Password”</i>	
	<i>“Time”</i>	
	<i>“Memory usage”</i>	
<i>“Configuration”</i>	<i>“Template”</i>	
	<i>“Edit”</i>	<i>“Operation devices”</i>
		<i>“Physical contacts”</i>
		<i>“Readers”</i>
		<i>“Card format”</i>
		<i>“Internal responses”</i>
<i>“Operating device control”</i>		
<i>“Access cards”</i>	<i>“Input”</i>	
	<i>“List”</i>	
	<i>“Load from file”</i>	
<i>“Events”</i>		
<i>“Status”</i>		
<i>“Diagnostic”</i>		

3. Working area of the page.

3. SETTING

3.1 Change of network setting of the controller

The controller has following configurations by default (they are specified in the certificate of the device and on the labels on the controller):

- MAC-address 00-25-0B-xx-xx-xx, where xx – is a number from 00 to FE;
- IP-address 10.x.x.x, where x – is a number from 0 to 254;
- Subnet mask 255.0.0.0.

To change network settings of the controller (only in user mode, Section 5.5 of Operation manual):

1. Click consistently in the Web-interface menu: **“Settings”** → **“Network”**. The page with working area will be opened:

IP-address: . . .
Mask: . . .
Gateway: . . .

2. In the input fields **“IP-address:”**, **“Mask:”**, **“Gateway:”** the new values of network Settings of the controller.
3. Click **“Save”** button. New network settings will be saved in the controller.

3.2 Setting of the access password of the controller

By default, access password of the controller is not specified. To change or set the new password:

1. Click in the Web-interface menu: **“Settings”** → **“Password”**. The page with working area will be opened:

New password:
Confirm password:

2. In the **“New password:”** field enter the new password of the controller, in the **“Confirm password:”** field enter the password again to confirm the correct input.
3. Click the **“Save”** button. The new password will be saved in the controller.

3.3 Change the system time of the controller

To change the time:

1. Click in the Web-interface menu: **“Settings”** → **“Time”**. The page with working area will be opened:

Change date: / /
Change time: : :
Synchronize with PC:

2. In the input fields “**Change Date:**”, “**Change Time:**” change the set values.
3. If necessary, put tick “**Synchronize with PC:**” to synchronize the time and date of the controller with the computer connected to the Web-interface.
4. Click the “**Save**” button.

3.4 Choice of Settings of memory allocation

By default, the controller memory is allocated to store data up to 50,000 access cards and up to 230,000 events. The user is able to change the memory allocation of the controller in accordance with the controller configuration. Other options of memory allocation:

- 10,000 cards and 870,000 events,
- 20,000 cards and 710,000 events,
- 30,000 cards and 550,000 events,
- 40,000 cards and 390,000 events.

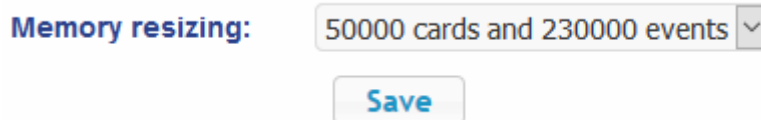


Note:

In software **PERCo-Web** are supported all these options, but their choice is only available in the Web interface.

To change Settings on the memory allocation of the controller:

1. Click in the Web-interface menu: “**Settings**” → “**Memory usage**”. The page with working area will be opened:



2. In dropdown list “**Memory resizing:**” select one of the variants of the memory allocation:
3. Click the “**Save**” button.

4. CONFIGURATION

4.1 The choice of the controller configuration

There is only one configuration template “**CL05.2 Controller**” available for **CL-05.2** controller. By default, controller is configured according to this template.



Attention!

If you change the configuration, the previous configuration and at the internal responses of all resources of the controller will be deleted. In the new template for the resources of the controller is installed default configuration. The list of downloaded access cards, related user information, rights and parameters of access remain the same.

To change the configuration of the controller:

1. Click in the Web-interface menu: “**Configuration**” → “**Template**”. The page with working area will be opened.
2. Press “**CL05.2 Controller**” template.
3. In the opened window click “**Continue**”. The controller configuration will be changed. Change the configuration template can take 30 seconds.

4.2 Configuration of the Settings of the controller resources

4.2.1 Operating devices

To configure Settings of the controller resources to control OD:

1. Click consistently in the Web-interface menu: **“Configuration”** → **“Edit”** → **“Operating devices”**. The page with working area will be opened:

Number	Operating device type
1	One-sided lock


2. To change Settings of the OD, click in the working area of the page on a line with his name (**“One-sided lock”**). The window with the OD name will appear:

3. In the opened window on the tabs **“General”**, **“Alarm generator”**, **“Reader 1”**, **“Operating device”** make the necessary changes of the Settings for corresponding resources.



Attention!

For the resource **“Reader 1”**, the parameter **“Card rights number”** indicates the number of the set of card rights used for passing with this reader. By default, value **“1”** is set everywhere for parameter **“Rights number”** and for correct operation of the controller it’s not recommended to change this value.

4. Click the **“Save”** button. The window will be closed, changed Settings will be passed to the controller.
5. To exit the window with the name of the OD without saving the changes, click the **“Cancel”** button or the **“Close”** button .

4.2.2 Physical contacts (inputs and outputs)

To configure the Settings of the controller inputs and outputs:

1. Click consistently in the Web-interface menu: **“Configuration”** → **“Edit”** → **“Physical contacts”**. The page with working area will be opened:

Contact	Function	Operating device	Direction	Normal
Input 1	Pass input	1	1	Closed
Input 2	Remote control	1	1	Cut
Input 3	Not specified			Cut
Output 1	Operating device control output	1	1	Not energized
Output 2	Not specified			Not energized

The page lists all the controller inputs and outputs.

By default, for inputs and outputs which are used for OD (lock) operation corresponding functions are set (for inputs – PASS / RC, for outputs – OD operation / RC-panel indication) and there are set number and direction of OD, to which current contact is connected.

For inputs and outputs which are not used for OD operation, by default, value **“Not specified”** is set. These outputs and inputs are available for setting (and changing in future) its functions.

Name in Web-interface	Function	Wire color
Input 1	Always – Door sensor, <i>Door (Pass)</i>	white
Input 2	Always – RC-button, <i>DU</i>	green
Output 1	Always – Lock operation, <i>Lock</i>	orange
Input 3 / Output 2	1) Input <i>Fire Alarm</i> , 2) Output <i>Alarm</i> (siren), 3) Input - output <i>SYNC</i> (synchronization of 2 controllers)	brown



Notes:

- *Input 3* or *Output 2* of **CL-05.2** controller are led in one leading-out wire – brown wire.
- “SYNC” function (synchronizing input-output for common operation of 2 **CL-05.2** controllers) for input 3 / output 2 can be set only via net software of PERCo systems (see Operating Manual, Section 5.4.3).
- It is possible to restore to factory default settings by resetting configuration template (see Clause 4.1).


2. Click in the working area of the page on the line with the name of the input (output). The window with the physical contact will be opened:

Physical contact Input 3
✕

Normal state: Closed

Function: [Not specified]

Save
Cancel

3. In the opened window make necessary changes of the Settings:
 - selector “**Normal state:**” defines the normal state of the contact – it is “**Opened**” or “**Closed**” for inputs or “**Energized**” and “**Not energized**” for outputs;
 - selector “**Function:**” sets the function of the contact.
4. Click the “**Save**” button. The window with the physical contact name will be closed, the changed Settings of inputs (outputs) will be passed to the controller.
5. To exit from the window of physical contact without saving changes, click the button “**Cancel**”. Also, it is possible to close the window using the “**Close**” button .

4.2.3 Reader

There is only one inbuilt reader in controller configuration template. Adding extra reader is impossible. This controller is designed to operate only one-sided door, operation of two-sided door is possible only with the help of two controllers, synchronized between each other for common operation (see Operating manual, Section 5.4.3).



Attention!

To avoid incorrect device operation do not change the settings of inbuilt reader #1, used for OD operation! If necessary, it is possible to restore to factory default settings by resetting configuration template (see Clause 4.1).

4.2.4 The reading format of the card identifiers



Attention!

- Change of this parameter when you have already entered the access control cards, results in the passage on these cards will be impossible.
- When connecting to the controller working under software of **PERCo** systems, the current format may not be shown (nothing is selected from the formats). In this case to change the reading format of card identifiers is **PROHIBITED**.

To select the reading format of card identifiers:

1. Click consistently in the Web-interface menu: “**Configuration**” → “**Edit**” → “**Card format**”. The page with working area will be opened:

Card reader operating mode: Wiegand 26 ▼

Save

2. Using the drop-down list “**Card reader operating mode**”: select one of offered formats and click the “**Save**” button.

4.2.5 Internal responses


To set internal responses of the controller:

1. Click consistently in the Web-interface menu: “**Configuration**” → “**Edit**” → “**Internal responses**”. The page with working area will be opened:

Add

Number	Source			Receiver		
	Type	Number	Direction	Type	Number	Direction
Data not found						

- To add the new response, click the **“Add”** button, to change the Settings of internal response or delete it, click in the working area of the page on the line with the response name. The window **“Internal response (number)”** will be opened:


- In the opened window make the necessary changes of the Settings:
 - Selector **“Number:”** sets the number of response (from 1 to 40).
 - Selector **“Source type:”** specifies the launch condition of the controller response.
 - Selector **“Source number:”** (**“Receiver number:”**) and **“Source direction:”** (**“Receiver direction:”**) determine numbers and directions of corresponding resources of the controller which are sources (receivers) of the response.
 - Selector **“Receiver type:”** specifies the controller response under condition of the responses launch.
 - Selector **“Response time:”** and **“Response characteristics:”** set corresponding Settings of the response.
- Click the **“Save”** button. The window **“Internal response (number)”** will be closed, the changed Settings will be passed to the controller.
- To remove the response from the list, click the **“Delete”** button. The window **“Internal response (number)”** will be closed, the internal response will be deleted.
- To exit the window Internal response (number) without saving changes, click the **“Cancel”** button. Also, it is possible to close the window using the **“Close”** button .

5. CONTROL OF OPERATING DEVICE

To control the operating device and change the operation mode in the direction with associated reader, make following:

- Click in the Web-interface menu: **“Operating device control”**.

- Click in the working area of the page on the line with OD "Lock #1". The control window with selected OD will be opened:

- Using the buttons at the bottom part of the window, give the necessary command. The control window will be closed; the command will be passed to the controller. To close the window without submitting command is possible with the "Close" button .



Note:

When you unlock the OD will be unblocked for the time chosen in the drop-down list "Unlock time".

6. ACCESS CARDS

6.1 Entering of the cards identifiers

To enter the card identifiers:

- Click consistently in the Web-interface menu: "Access cards" → "Enter". The page with working area will be opened:

- If necessary, use the dropdown list in the heading of the "Number type" column, select the format to display the cards identifiers.



Note:

The display format is not the format of reading of the card identifiers (set in the "Configuration" section, Clause 4.2.4), when you change the display format, the format of reading does not change.

- Entering of the card identifiers from the reader:
 - In the working area of the page click the "Switch on card reader input" button.
 - Present your card to one of the readers included in the controller configuration. The card identifier will appear in the working area of the page. Also, you will see the buttons "Save" and "Load to emergency list".

- If necessary, similarly add other cards.

Number type

139,46934

48,22984

37,46820

2,42291

- In the working area of the page click the **“Switch off card reader input”** button.

4. Entering of the card identifiers manually:

- In the working area of the page click the **“Manual input”** button. The window **“Card input”** will be opened:

Card input ✕

Card number:

- In the **“Card number:”** field enter the card identifier. Click the **“Save”** button. The window **“Card input”** is closed; the card identifier appears in the working area of the page.

- If necessary, similarly, add the other cards.

5. To transfer the entered card identifiers to the controller, click the **“Save”** button in the working area of the page. The identifiers will be transferred to the main list of the cards in section **“List”**.



Attention!

When you enter the card identifiers in the list of the controller, by default they are granted rights of access over all ODs connected to the controller (all 12 sets of rights for each card have the status **“Unblocked”**), Clause 6.2.

6.2 The list of stored cards

To work with the list of the cards stored previously in the controller’s memory:

1. Click consistently in the Web-interface menu: **“Access cards”** → **“List”**. The page with working area will be opened:

Number	Valid till	Type	Full name
<input type="text" value="Wiegand 26"/> <input type="button" value="v"/> 1,19	18-07-2017 18:00:59	Temporary	Kravtschuk Sergey
56,15714	24-07-2019	Permanent	Savitskiy A.P.
190,50942	25-07-2019	Permanent	Gritovt Peter
243,50788	18-07-2017 18:00:59	Temporary	Visitor #1

- If necessary, use the dropdown list in the heading of the **“Number”** column, select the format to display the cards identifiers.

**Note:**

The display format is not the format of reading of the card identifiers (set in the **“Configuration”** section, Clause 4.2.4), when you change the display format, the format of reading does not change.

- To save the cards to a file, click the **“Save file”** button. The cards will be saved in the file `cards.bin`, which can be used as a backup card list.
- To remove all the cards from the controller memory, click the **“Clear log”** button.
- To change the Settings, select one of the cards in the working area of the page. The window of the identifier of the selected card opens:

1,19

General Access rights

Card type: Temporary

Valid from: 18/07/2017 Hour: 11 Min.: 15

Valid till: 18/07/2017 Hour: 18 Min.: 0

Stop list: No

Vehicle card: No

Full name: Kravtshuk Sergey

Delete Save Cancel

- If necessary, in the opened window on the **“Essential”** tab change the card Settings.
- Go to the **“Access rights”** tab. It is possible to set access rights for this card. To do this, select the number of the set using the drop-down list **“Card rights number:”** and configure the Settings:

1,19

General Access rights

Card rights number: 1

Access time interval: Time zone

Time criteria number: 2

Guard zone number: 1

Access permission: Permitted

Other cards commissioning: No

Antipassback: Yes

Verification: Yes

Status: Unblocked

Delete Save Cancel



Attention!

Rights number, set for the card, should correspond to parameter “**Card rights number:**” of “**Reader**” resource, set in section “**Configuration**” → “**Edit**” → “**Operation devices**”. By default, value “**1**” is set everywhere for parameter “**Rights number**” and for correct operation of the controller it’s not recommended to change this value.

8. To delete the card, click the “**Delete**” button at the bottom part of the window.
9. To save changed Settings of the card, click the “**Save**” button. The window will be closed, changed Settings will be passed to the controller.

The Settings of the set of access rights correspond to similar Settings in network software of **PERCo** systems.



Attention!

Setting of Settings of time access criteria via the controller is possible only in network software of **PERCo** systems. In the Web-interface is only possible to change the time criterion (time zone, weekly schedule, flexible daily schedule, flexible weekly schedule) and transition from one set of time Settings to another set by changing his number. The number of time criterion corresponds to order number of the set of Settings of time criterion in the network software.

6.3 Loading the identifiers from a file

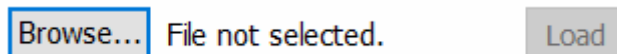


Attention!

When loading the list of cards from the file to the controller, previously loaded cards are deleted automatically from the controller memory.

The list of the cards can be loaded only from the file `cards.bin`, created via Web-interface of the controller earlier. To download the numbers of the card from a text file:

1. Click consistently in the Web-interface menu: “**Access cards**” → “**Load from file**”. The page with working area will be opened:



2. Click the “**Browse...**” button. In the opened window of the Explorer specify location and name of the file with the card list and click the “**Open**” button. The explorer window will be closed; the file name will be indicated in the field near the “**Browse...**” button.
3. Click the “**Load**” button. The window “**Progress**” will be opened containing information about the boot process.



7. EVENTS

To view the event log of the registration of the controller:

1. Click in the Web-interface menu: **“Events”**. The page with working area will be opened:

Date	Event
07/11/17 09:36:22	Recovery of internal power supply +5V
07/11/17 09:36:22	FireAlarm entrance normalization
07/11/17 09:36:22	Switch on the controller
03/11/17 16:45:14	Switch off the controller

[Filter](#)

[Save](#) [Clear](#)

[<< First](#)
[< Earlier](#)
[Later >](#)
[Last >>](#)

2. By default, all events stored in the controller memory are displayed, by 20 events on the page. To move through the pages of the event, use the buttons located in the lower part of the working area. The events in the working area of the page are displayed in reverse chronological order.
3. There is possibility of selection in the report of events by categories and time. To do this, click the **“Filter”** button, the window **“Filter”** will be opened:
4. In the dropdown list **“Selected categories: [number]”** put ticks the event categories which should be reported. Following categories of events are available:
 - **“ID Card access”**
 - **“Guard zone status change”**
 - **“Guard zone resource state change”**
 - **“Change input/output state change”**
 - **“Access without ID Card”**
 - **“Functioning”**
5. Use the fields **“Range beginning point”** and **“Range end point”** to set the period of the report.
6. Click the **“Apply”** button to apply the filter, click the **“Cancel”** button to cancel any made changes. The window **“Filter”** closes, the report will display the events in accordance with the filter settings.
7. To save the events to a file, click the **“Save”** button at the bottom part of working area of the page. The events will be saved in the file `events.txt`.
8. To delete all events from the controller memory, click the **“Clear”** button at the bottom part of working area of the page.

8. STATUS

To view the controller status and status of all his resources click in the Web-interface menu “**Status**”. The page with working area will be opened:

Object	Status
Hardware error	Missing
Device mode	Working state
Status	Ok
Alarm Operating device №1	Off
Output 1	Off
Input 1	Off
Reader access control mode 1	Control
Operating device №1	Disarmed, Ok, Blocked
Guard zone 1	Disarmed
Jumper IP_MODE	off
Jumper IP_DEFAULT	off

9. DIAGNOSTICS

For diagnostics and maintenance of the controller:

1. Click in the Web-interface menu: “**Diagnostic**”. The page with working area will be opened:

Diagnostics (50 min):

Diagnostics with formatting (15 min):

Formatting (2 min):

Software update: File not selected.

2. To start testing the status of the controller hardware click the “**Start**” button in the line “**Diagnostics (50 min):**”. In the confirmation window click “**OK**”.



Attention!

When testing the controller, the event log is automatically cleared.

3. For diagnostic purposes of the controller with the previous formatting, click the “**Start**” button in the line “**Diagnostics formatting (15 min):**”.
4. To start formatting the internal memory of the controller, click the “**Start**” button in the line “**Format (2 min):**”. In the confirmation window click “**OK**”.



Attention!

When formatting the controller memory, the information about configuration, access cards, time and area zones, controller password and events in the event log is automatically cleared.

5. To update the controller software (firmware), indicate the location of the software file using the “**Browse**” button and click the “**Update**” button.

PERCo

Polytechnicheskaya str., 4, block 2
194021, Saint Petersburg
Russia

Tel: +7 812 247 04 64

**E-mail: export@perco.com
support@perco.com**

www.perco.com



www.perco.com